REMARKS

Reconsideration and allowance are respectfully requested.

A typographical error is corrected in the independent claims. New dependent claims 50 and 51 are added and find example support at page 10, lines 27-30.

Claims 24-26, 28, 29, 32, 33, 35-37, 39, 40, 43, 44, and 46 stand rejected under 35 U.S.C. §103 as allegedly being unpatentable based on D'Argence in view of newly-applied Bhagwat et al. (US Publication No. 20050128989). This rejection is respectfully traversed.

In the claimed technology, access relevant information upon which resource management decisions are based is extracted by sniffing messages sent within an access network. As a result, existing internal interfaces are used to obtain the access relevant information making it is easier to expand a communications system with a new access network using a new access technology. In other words, it is not necessary to standardize new specific interfaces between the new access network units and a common radio resource manager for reporting access relevant information to the common radio resource manager. Instead, the common radio resource manager obtains the access relevant information from sniffing on the internal interfaces within the new access network as explained in the application.

D'Argence discloses a communication system comprising a common radio resource manager (CRRM) that coordinates the use of the radio resources from different radio access systems. The CRRM receives information required for the CRRM to perform the resource management algorithms from network elements. In contrast to the claims, D'Argence defines specific interfaces and dedicated signaling between network entities and the CRRM in order to provide the CRRM with the information it requires (see D'Argence, page 8, line 9-24). Moreover, the CRRM function makes specific requests to relevant network entities for the

information it requires (see page 16, line 8-18). As a result, there is no need in D'Argence to sniff messages sent within an access network to obtain the required information.

The Examiner therefore correctly admits that D'Argence lacks multiple features from the independent claims in the office action in the paragraph bridging pages 3 and 4. For these missing features, the Examiner turns to Bhagwat which concerns a method and a system for intrusion detection in wireless systems. A sniffer 122 is used to monitor wireless activity in an airspace in order to make it possible to detect a violation of a security policy. The sniffer is used to protect against an unauthorized wireless activity, e.g., an unauthorized AP masquerading as an authorized AP which may also be luring authorized clients to connect to it, thereby creating another level of legitimacy to further elude detection. The security policy can characterize a type of wireless activity in the unsecured airspace to be permitted, denied, or ignored.

There is no disclosure in Bhagwat of a communication system with a plurality of access networks using different access technologies, and thus, no disclosure of determining which access network provides the best connection to a terminal.

The proposed combination of D'Argence and Bhagwat does not teach claims 24, 35, and 46. That combination leads to a system having specific interfaces between access network units with network entities reporting access relevant information to D'Argence's CRRM with a security system including sniffers like that described in Bhagwat. But the additional of Bhagwat sniffers in system of D'Argence simply improves security. A security sniffer does not affect the management of radio resources of the system or how an appropriate access network is determined for a terminal. In claim 24, for example, how is the security sniffer in D'Argence's system "determin[e] which access network that provides a best connection to a terminal and which access network should be accessed, based on at least a result of the comparison of the

1556636

received access relevant information extracted from messages sent within the first access network to the access relevant information received from the at least one second access network"?

Also, Applicants do not understand the Examiner's stated reason for combining D'Argence with Bhagwat: "to achieve the goal of removing only the desired configuration information from a packet in a communication system." How does a security sniffer achieve this goal in D'Argence?

Regarding claims 29 and 40, the Examiner relies on D'Argence for the feature "wherein at least part of the access relevant information is extracted by sniffing user plane traffic for at least one terminal, which access relevant information is used to calculate traffic volume and/or throughput of the at least one terminal." But the Examiner admitted that D'Argence does not teach the claimed listening agent sniffing user plane traffic including a source and destination address and data payload of a sniffed message. Page 13, lines 24-29 simply describe that a user plane exists with no reference to sniffing. Nor does page 19, lines 1-3 describe sniffing user plane traffic to obtain information to calculate traffic volume or throughput of a terminal. D'Argence has to request that special messages be sent directly to the CRRM rather than sniffing existing messages.

Similar deficiencies are present for claims 33 and 44 which recite "wherein at least part of the access relevant information extracted by sniffing messages sent within the first access network indicates how frequently a channel was busy, which indicates a load of the channel." Page 4, lines 10-11 of D'Argence does not relate the "dynamic information" to any sort of sniffing existing messages.

1556636

The subject matter of claims 50 and 51 also appears missing from the applied references. Claim 51 recites for example "wherein when the access relevant information is expressed in non-comparable quantities, the method further comprises converting access relevant information from at least one of the first and second access networks to an access-independent quantity before performing the comparison of the access relevant information extracted from the first access network to the access relevant information received from the at least one second access network." Conversion of the claimed sniffed access relevant information is not believed taught in D'Argence or Bhagwat.

Accordingly, the application is in condition for allowance. An early notice to that effect is requested.

Respectfully submitted,

NIXON & VANDERHYE P.C.

By: _____

John R. Lastova
Reg. No. 33,149

JRL:maa
901 North Glebe Road, 11th Floor
Arlington, VA 22203-1808
Telephone: (703) 816-4000
Facsimile: (703) 816-4100

1556636